

Prior Art
Figure 2. Example of SMTP Message Transfer

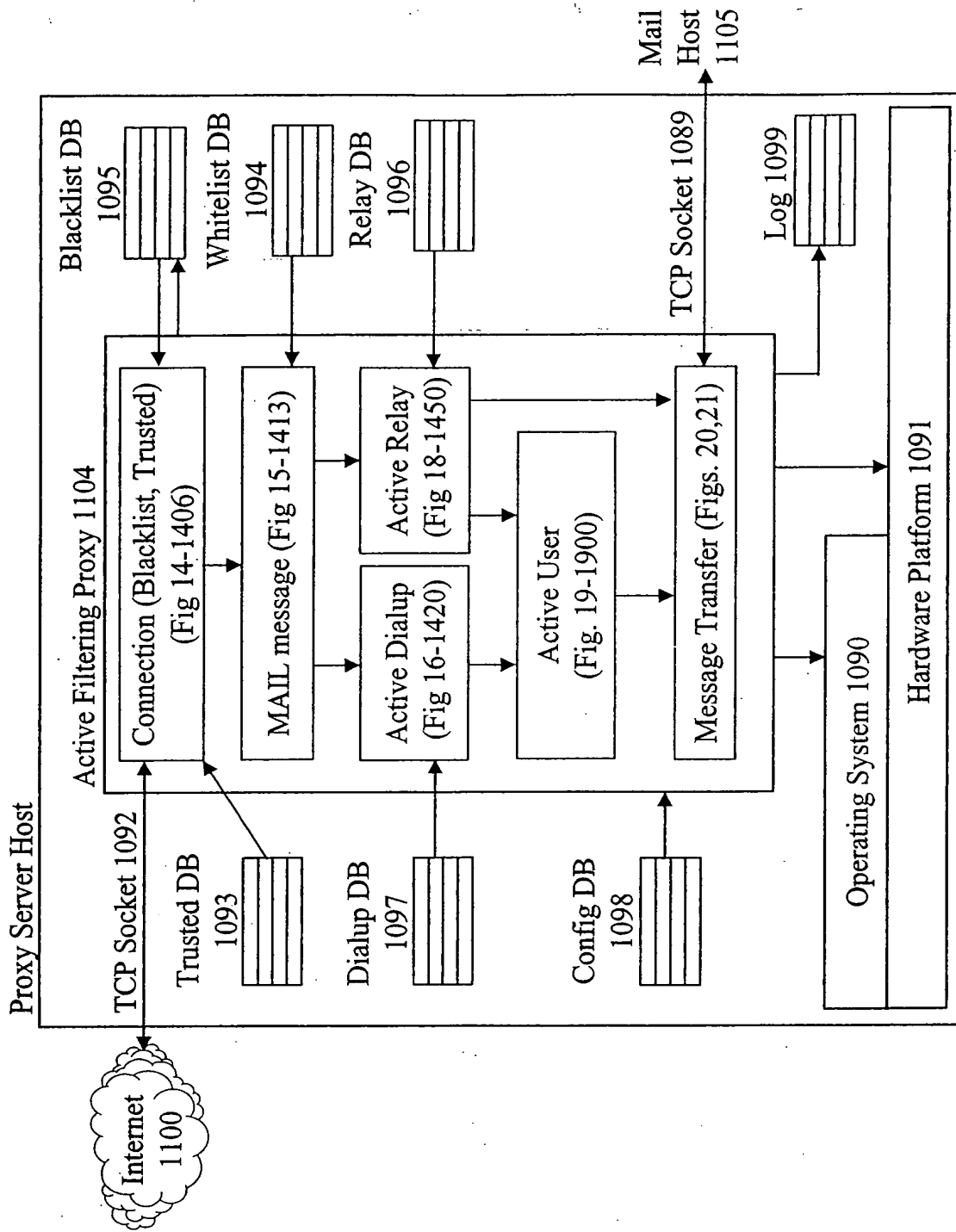


Figure 7. Block Diagram of Active Filtering System

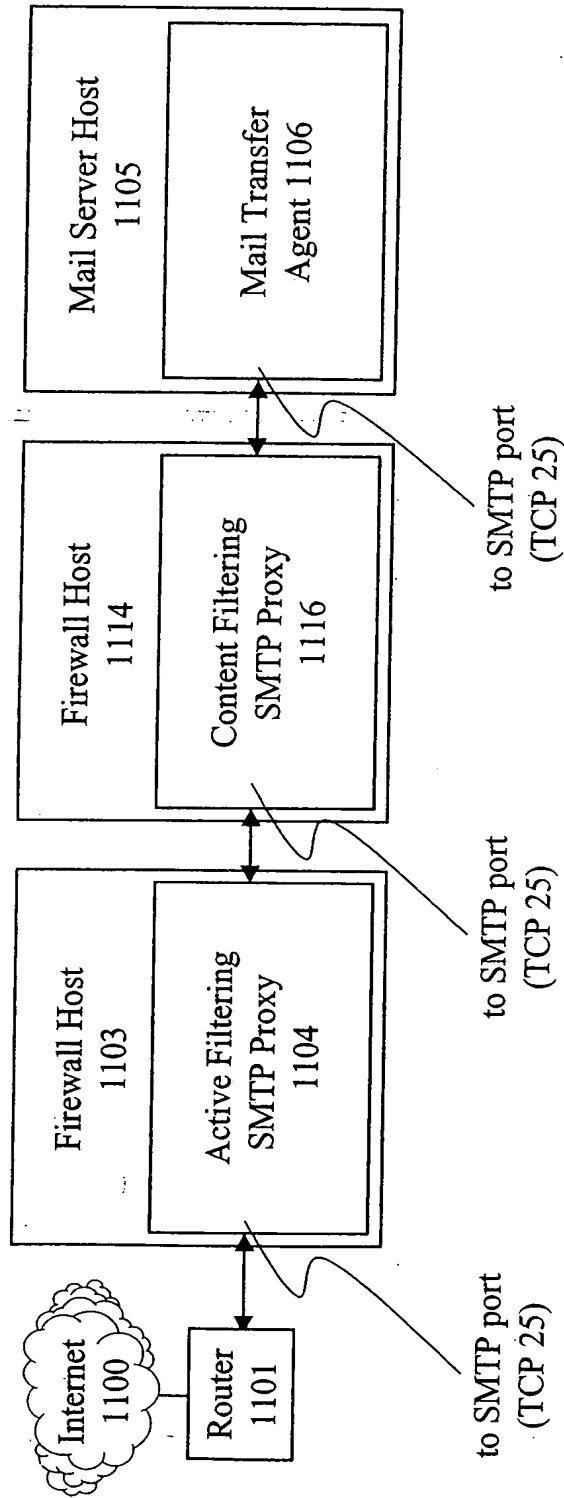


Figure 12. Active Filtering Proxy chained with Content Filtering Proxy

Remote 1400

1403
1410
1413

1480
1484
1488
1493
1495

TCP connection to proxy
HELO
MAIL From:
Reverse TCP connection

HELO
MAIL From:
RCPT To:

Active Filter Proxy 1401

1406 IP Blacklist Filter (Fig. 14)
(Fig. 15)
1418 Open connection (Fig. 15)
(Fig. 15)
1420 Active Dialup (Figs. 16-17)

1450 Active Relay (Fig. 18)

1901 Active User (Fig. 19)

RCPT To:
DATA
Message header
Message body
dot, quit

TCP connection to MTA
HELO
MAIL From:

1470
1472
1474
Fig. 20
Fig. 21
1491 Bcc Filter

Local MTA 1402



Figure 13. Active Filtering Overview (not showing status responses or error conditions)

Remote 1400

1403

TCP connect to SMTP port

Active Filter Proxy 1401

get remote address, name 1404

trusted host? 1405

no

match

entry in blacklist DB? 1406

yes

550 SMTP blocked

send error response
close connection
log rejection
exit 1408

220 greeting

send greeting 1409

Local MTA 1402



Figure 14. IP Blacklist Filtering

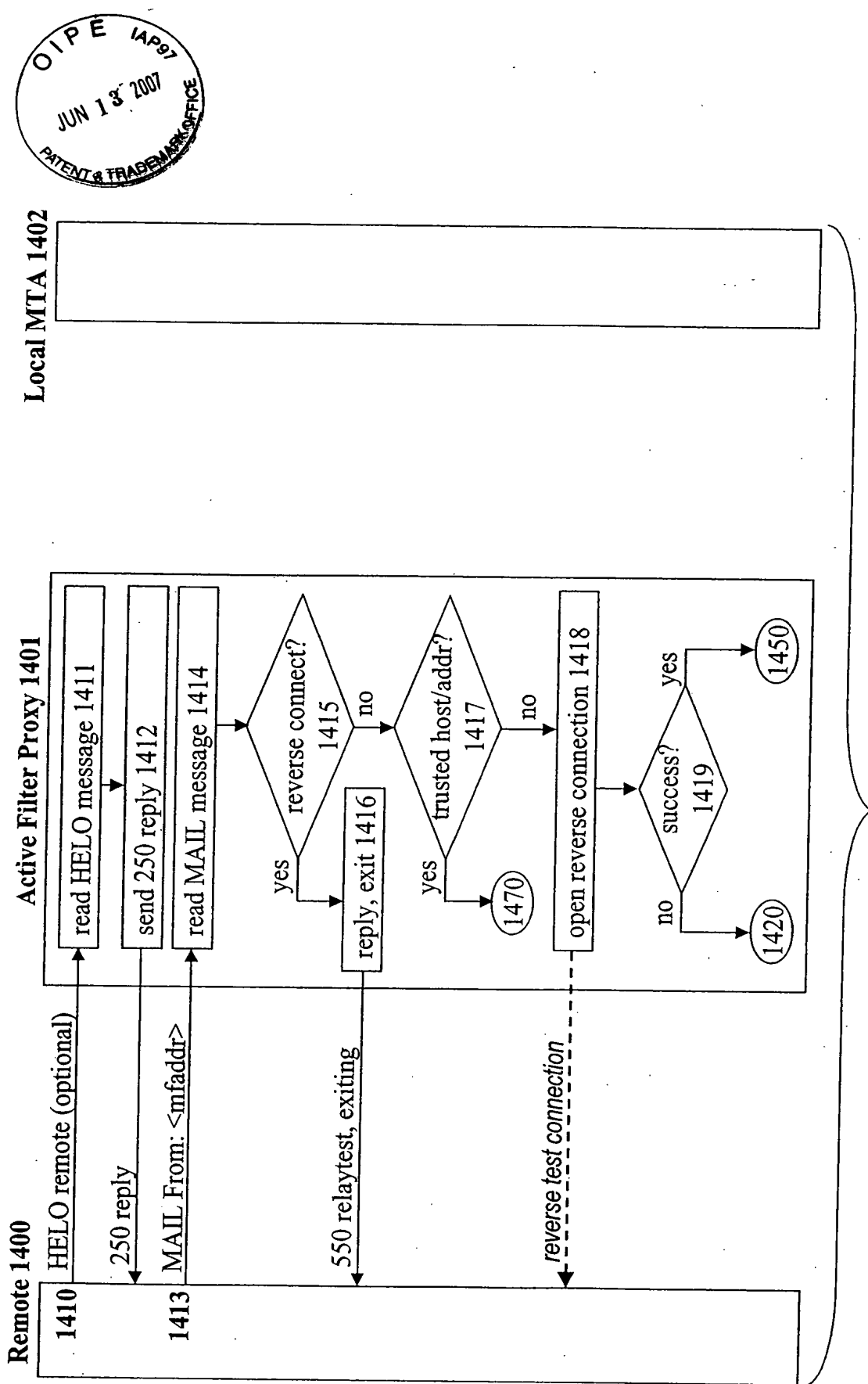


Figure 15. Remote HELO and MAIL Message Processing

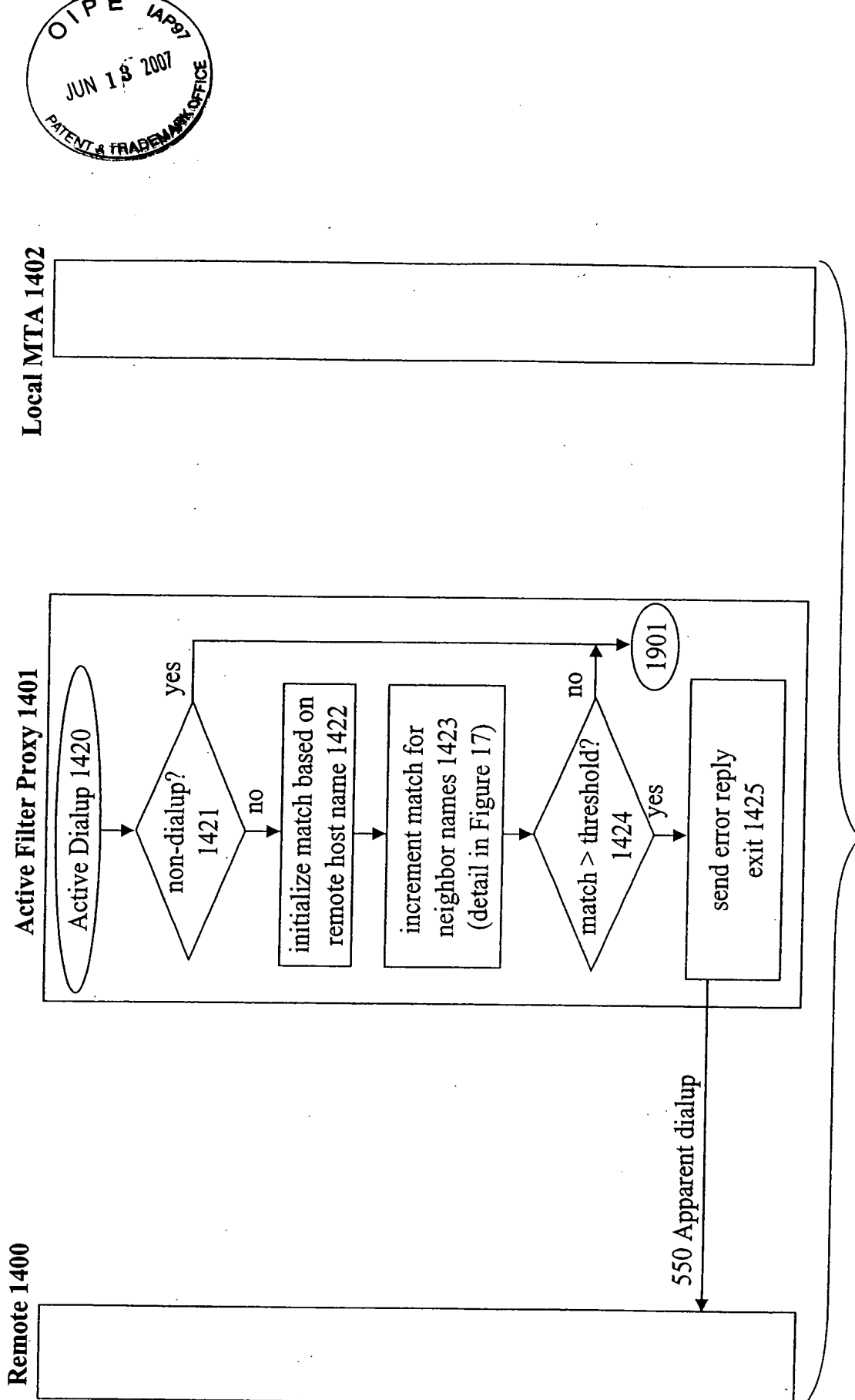


Figure 16. Active Dialup Test



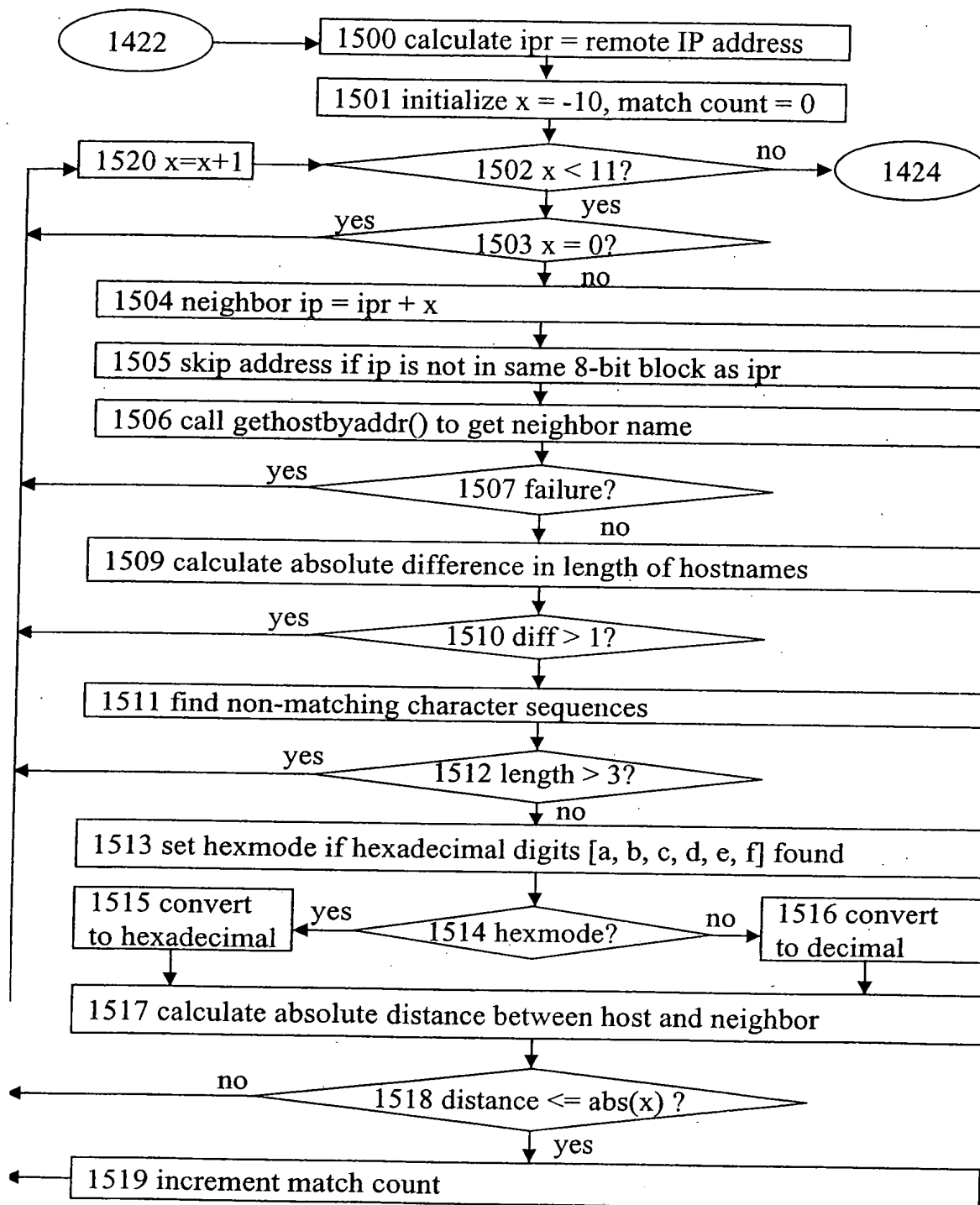


Figure 17. Details of Figure 16 Step 1423

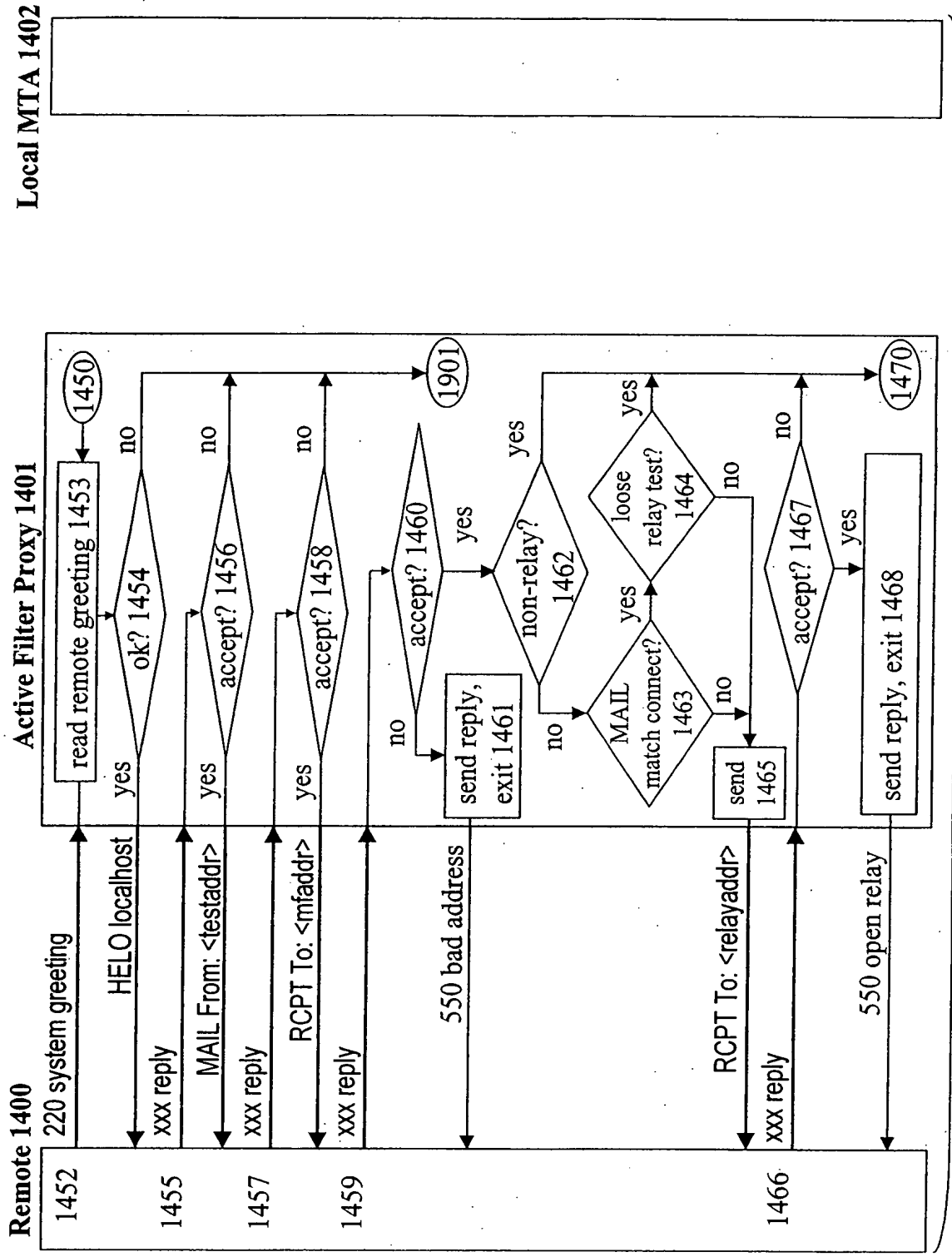


Figure 18. Active Relay Test



Local MTA 1402

Active Filter Proxy 1401

Mailhost 1900

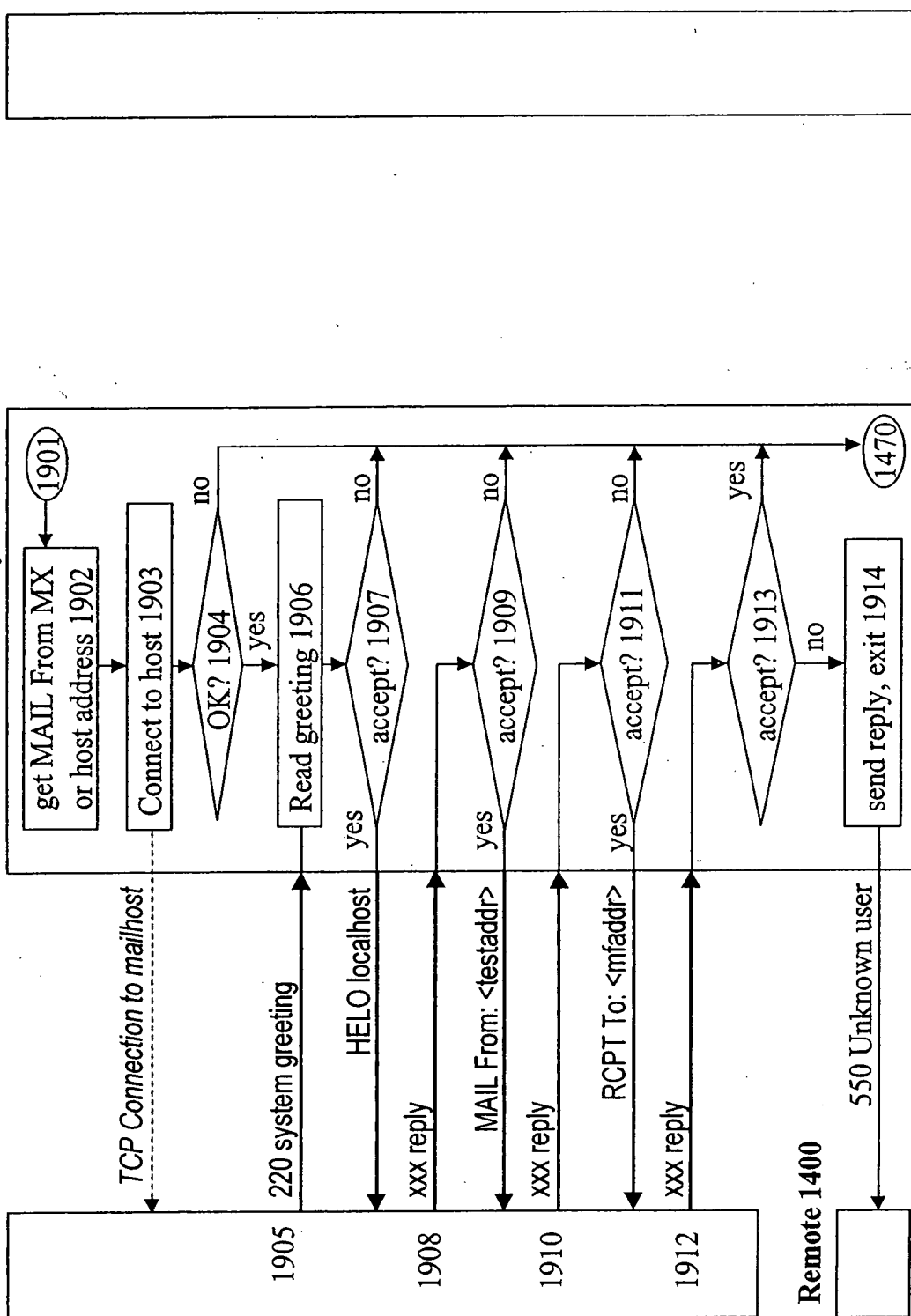


Figure 19. Active User Test

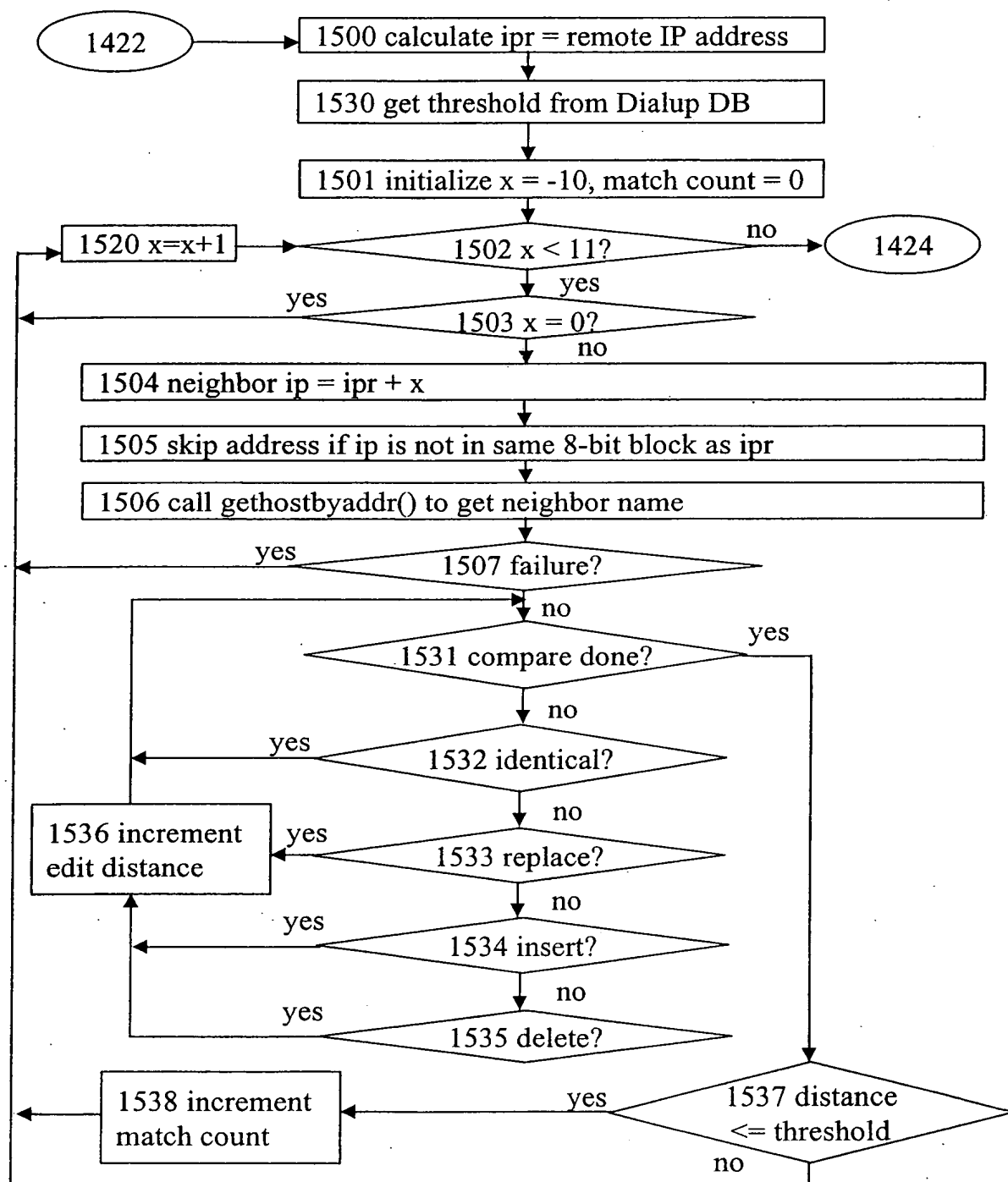


Figure 22. Details of Edit Distance Method
(Alternative Figure 16 Step 1423)

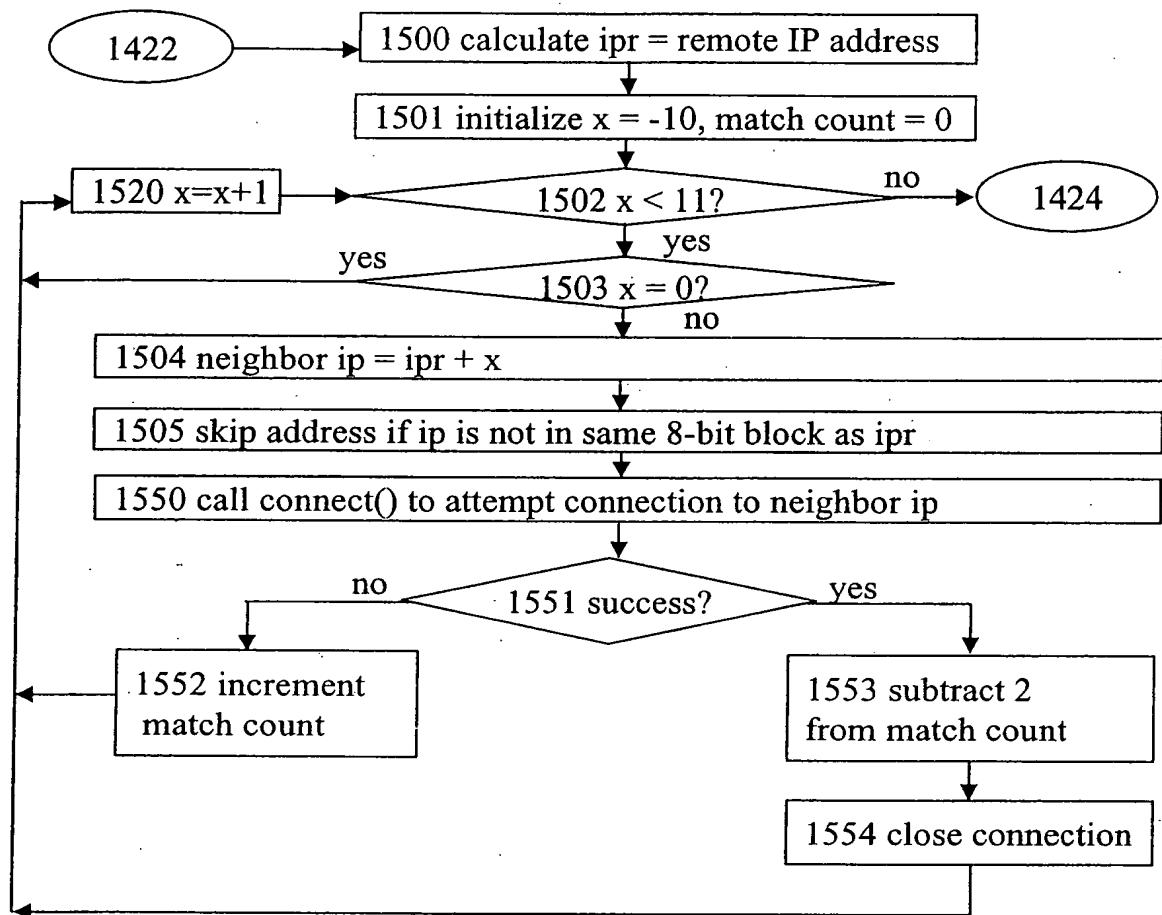


Figure 23. Details of Neighbor Connection Method
(Alternative Figure 16 Step 1423)

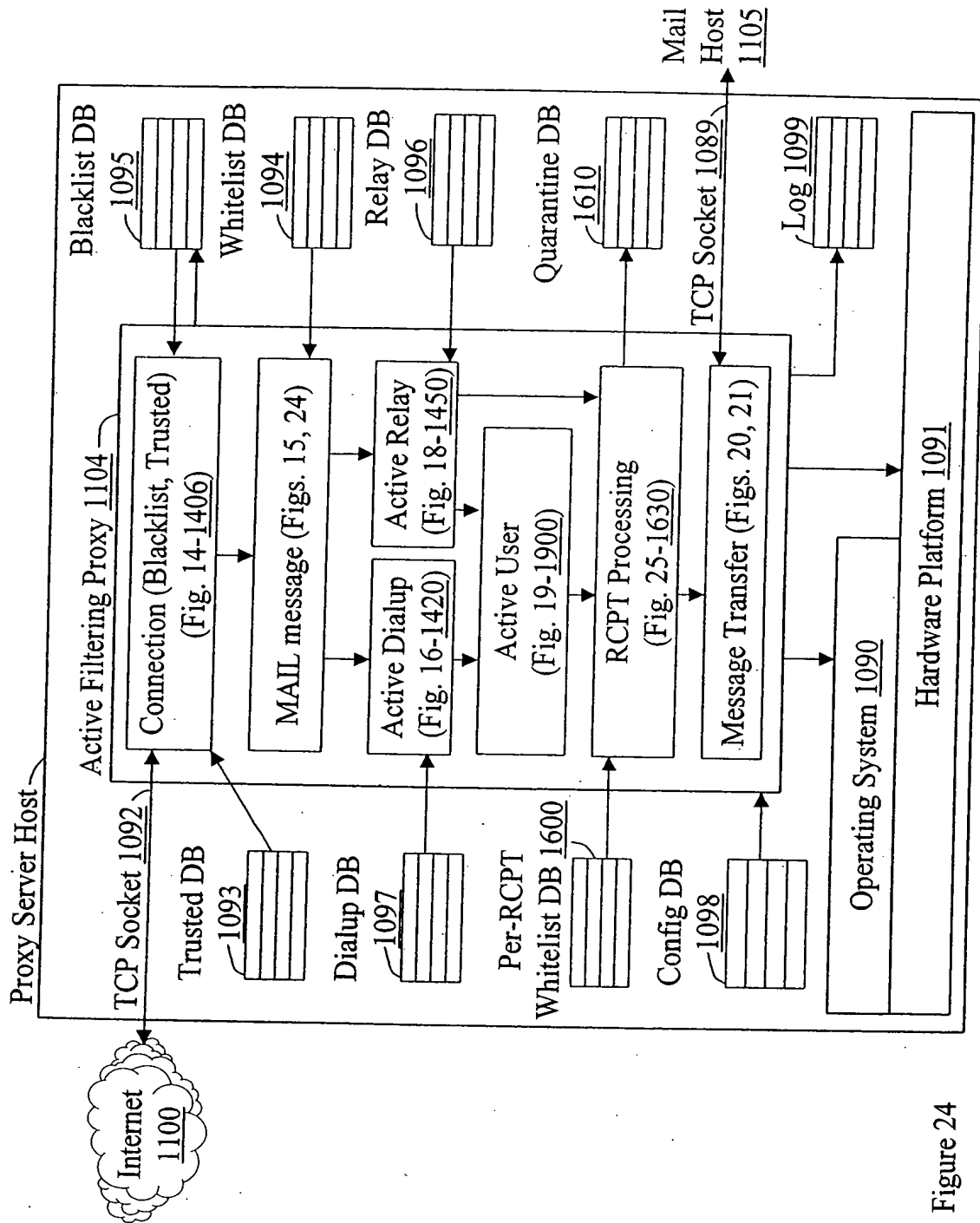


Figure 24

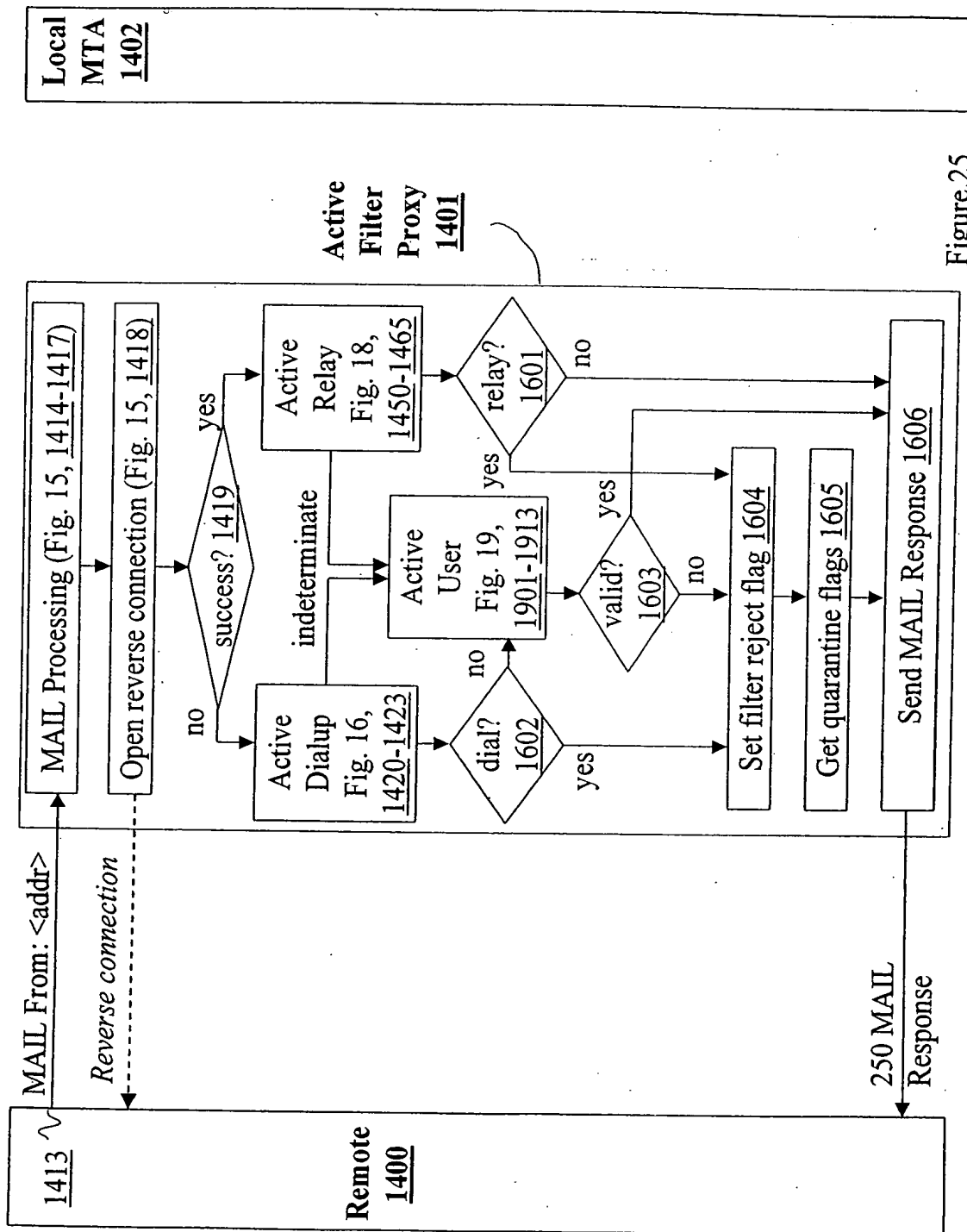
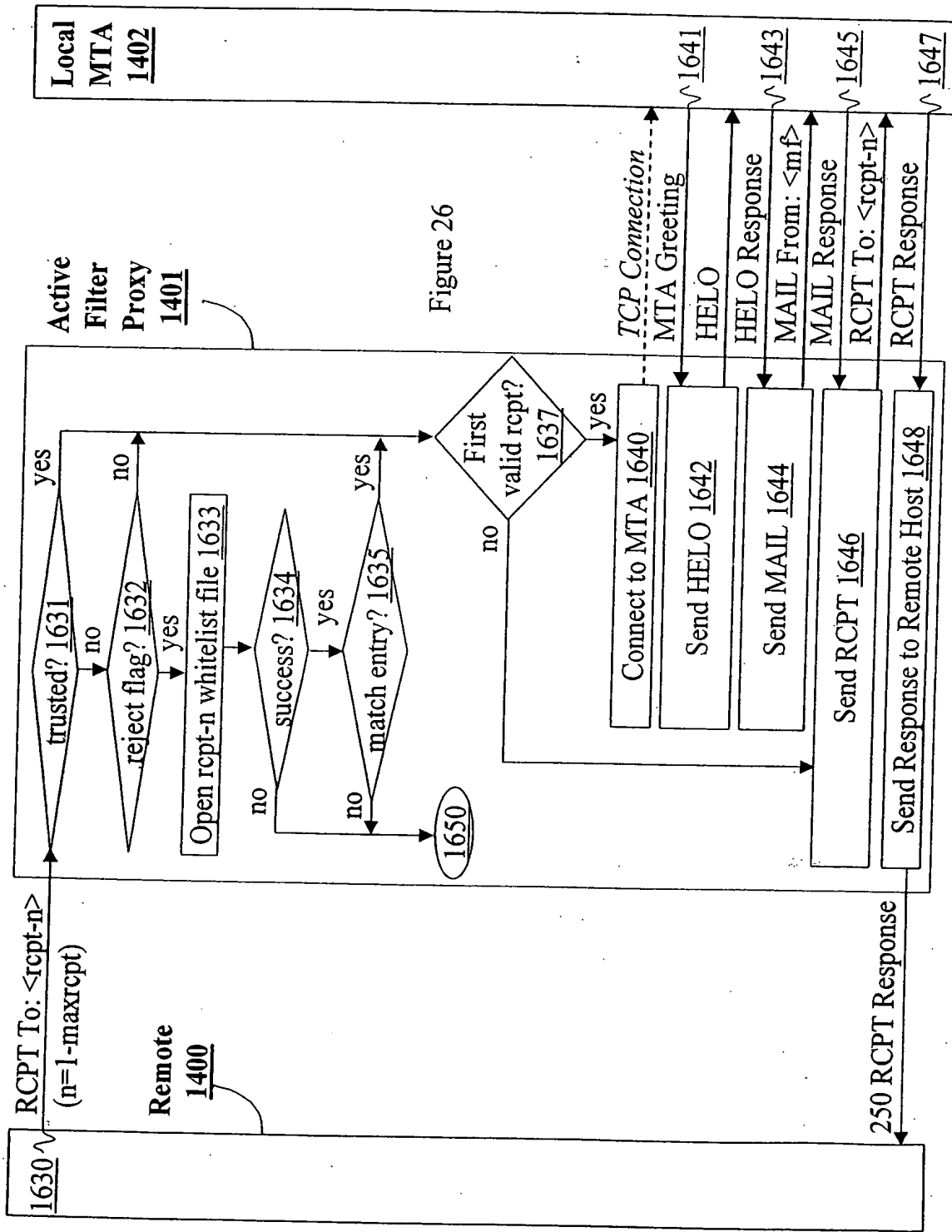


Figure 25



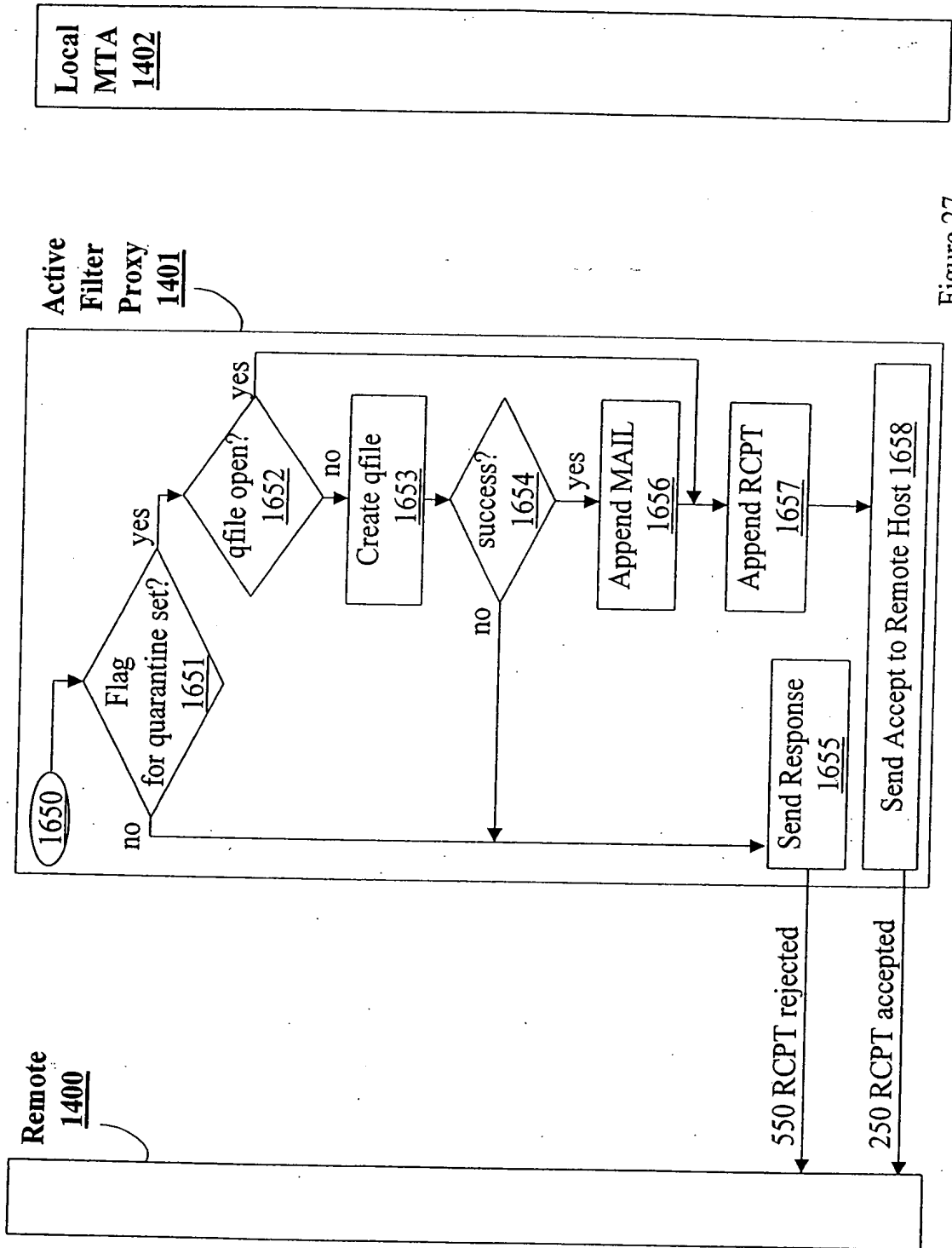


Figure 27

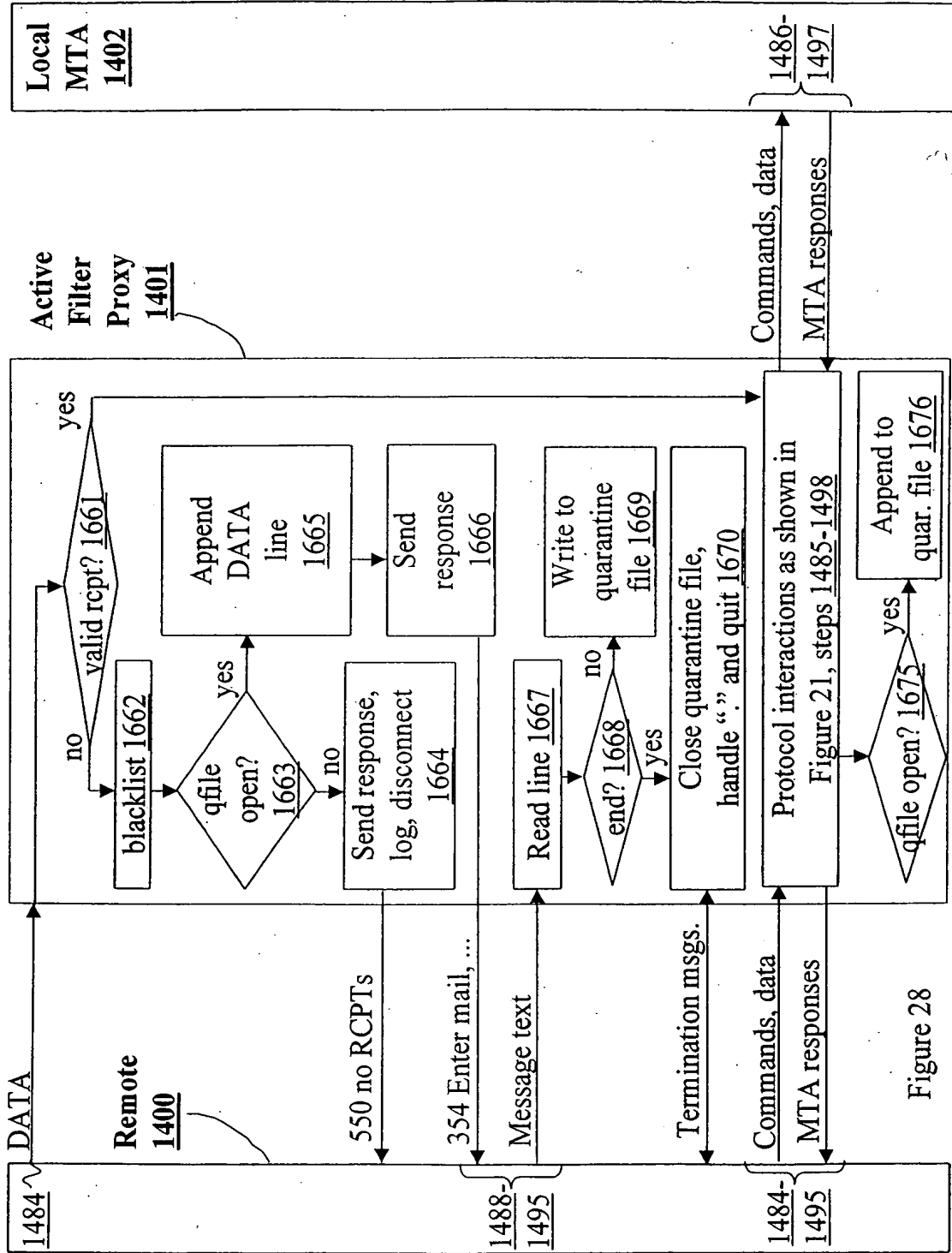


Figure 28

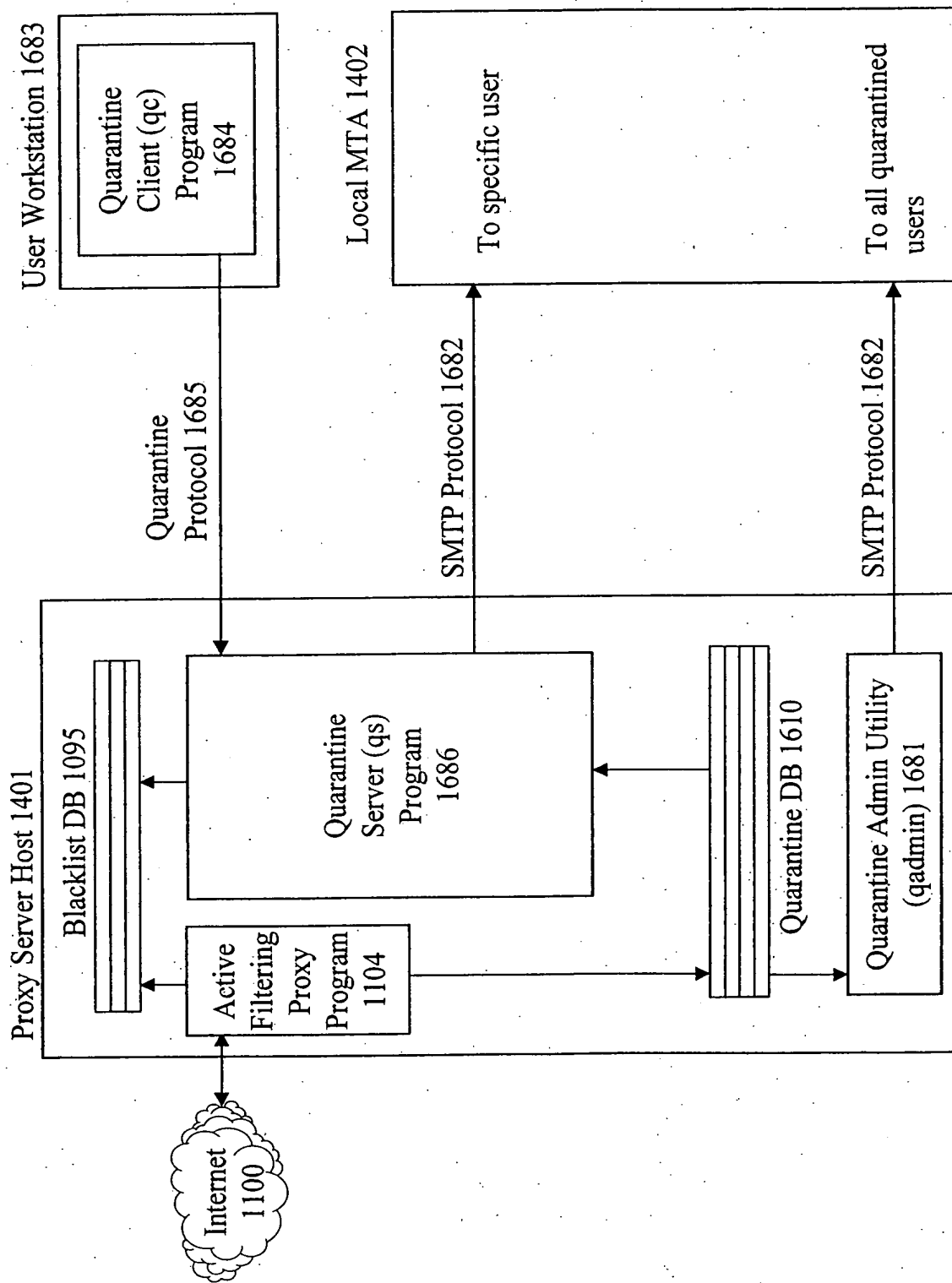


Figure 29. Quarantined Message Retrieval